日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月２０日

出願番号
Application Number: 特願２０００－０１４１９５

出願人
Applicant (s): ソニー株式会社

２０００年１１月１７日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９５９０７

【書類名】　特許願

【整理番号】　00000226

【提出日】　平成12年 1月20日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 13/00

H04H 1/00

【請求項の数】　52

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　平井　純

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　062721

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ提供システム及びコンテンツ提供方法、コンテンツ提供状況監視装置及び監視方法、並びに、コンテンツ使用装置及び使用方法

【特許請求の範囲】

【請求項１】

所定の権利者が所有するコンテンツを提供するためのコンテンツ提供システムであって、

コンテンツの使用許諾を示す認証情報を発行してコンテンツの提供を監視する監視装置と、

前記監視装置から受け取った認証情報を付けてコンテンツを所定の配布路経由で提供する配布装置と、

を具備することを特徴とするコンテンツ提供システム。

【請求項２】

前記監視装置は、前記所定の配布路上で提供中のコンテンツを取得して、該コンテンツに認証情報が付されているか否かで配布装置によるコンテンツ提供行為の正当性を判断することを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項３】

前記監視装置は、現在時刻を示す時刻識別情報と配布装置に対して割り当てた配布者識別情報の組を認証情報として発行することを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項４】

前記監視装置は、認証情報に加えて暗号鍵を発行し、

前記配布装置は、前記監視装置から受け取った暗号鍵を用いて暗号化した認証情報を付けてコンテンツを前記所定の配布路経由で提供する、

ことを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項５】

前記配布装置は、電子透かし技術を用いて認証情報をコンテンツに埋め込むことを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項６】

前記配布装置は、電子透かし技術を用いて認証情報をコンテンツの配布信号に埋め込むことを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項７】

各コンテンツは固有のコンテンツ識別情報を有し、

前記配布装置は、前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存することを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項８】

各コンテンツは固有のコンテンツ識別情報を有し、

前記配布装置は、前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存するとともに、該提供履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを渡すことを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項９】

各コンテンツは固有のコンテンツ識別情報を有し、

前記配布装置は、前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存し、

前記監視装置は、該提供履歴を基に各コンテンツの提供状況を管理することを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項１０】

各コンテンツは固有のコンテンツ識別情報を有し、

前記配布装置は、前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存し、

前記監視装置は、該提供履歴をアドレス可能な識別情報を前記認識情報に含めることを特徴とする請求項１に記載のコンテンツ提供システム。

【請求項１１】

所定の権利者が所有するコンテンツを提供するためのコンテンツ提供方法であって、

コンテンツの使用許諾を示す認証情報を発行する第１のステップと、

前記第１のステップにおいて発行された認証情報を付けてコンテンツを所定の配布路経由で提供する第２のステップと、

前記配布路上におけるコンテンツの提供を監視する第３のステップと、

を具備することを特徴とするコンテンツ提供方法。

【請求項１２】

前記第３のステップでは、前記所定の配布路上で提供中のコンテンツを取得して、該コンテンツに認証情報が付されているか否かでコンテンツ提供行為の正当性を判断することを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１３】

前記第１のステップでは、現在時刻を示す時刻識別情報とコンテンツ配布に対して割り当てた配信者識別情報の組を認証情報として発行することを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１４】

前記第１のステップでは、認証情報に加えて暗号鍵を発行し、

前記第２のステップでは、前記第１のステップにおいて発行された暗号鍵を用いて暗号化した認証情報を付けてコンテンツを前記所定の配布路経由で提供する、

ことを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１５】

前記第２のステップでは、電子透かし技術を用いて認証情報をコンテンツに埋め込むことを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１６】

前記第２のステップでは、電子透かし技術を用いて認証情報をコンテンツの配布信号に埋め込むことを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１７】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、前記第２のステップにおいて前記所定の配信路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存する第４のステップを

具備することを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１８】

各コンテンツは固有のコンテンツ識別情報を有し、さらに、

前記第２のステップにおいて前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存する第４のステップと、

該提供履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを抽出する第５のステップと、

を具備することを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項１９】

各コンテンツは固有のコンテンツ識別情報を有し、さらに、

前記第２のステップにおいて前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存する第４のステップと、

該提供履歴を基に各コンテンツの提供状況を管理する第６のステップと、

を具備することを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項２０】

各コンテンツは固有のコンテンツ識別情報を有し、さらに、

前記第２のステップにおいて前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存する第４のステップを具備するとともに、

前記第１のステップでは該提供履歴をアドレス可能な識別情報を含めて認証情報を発行する、

ことを特徴とする請求項１１に記載のコンテンツ提供方法。

【請求項２１】

所定の権利者が所有するするコンテンツの使用を監視するためのコンテンツ監視装置であって、コンテンツ使用者に対して使用許諾を示す認証情報を発行する手段を具備することを特徴とするコンテンツ監視装置。

【請求項２２】

前記認証情報は、少なくとも、現在時刻を示す時刻識別情報と、配布者に対して割り当てた配布者識別情報を含むことを特徴とする請求項２１に記載のコンテ

ンツ監視装置。

【請求項２３】

前記認証情報は、少なくとも、配布者に対して割り当てた配布者識別情報と、該配布者におけるコンテンツの提供履歴をアドレス可能な識別情報を含むことを特徴とする請求項２１に記載のコンテンツ監視装置。

【請求項２４】

認証情報に加えて暗号鍵を発行することを特徴とする請求項２１に記載のコンテンツ監視装置。

【請求項２５】

さらに、使用中のコンテンツを取得して認証情報の有無を検査する手段を具備することを特徴とする請求項２１に記載のコンテンツ監視装置。

【請求項２６】

さらに、コンテンツ使用者のコンテンツ使用履歴を基にコンテンツ使用状況を管理する手段を具備することを特徴とする請求項２１に記載のコンテンツ監視装置。

【請求項２７】

所定の権利者が所有するするコンテンツの使用を監視するためのコンテンツ監視方法であって、コンテンツ使用者に対して使用許諾を示す認証情報を発行することを特徴とするコンテンツ監視方法。

【請求項２８】

前記認証情報は、少なくとも、現在時刻を示す時刻識別情報と配布者に対して割り当てた配布者識別情報を含むことを特徴とする請求項２７に記載のコンテンツ監視方法。

【請求項２９】

前記認証情報は、少なくとも、配布者に対して割り当てた配布者識別情報と、該配布者におけるコンテンツの提供履歴をアドレス可能な識別情報を含むことを特徴とする請求項２７に記載のコンテンツ監視方法。

【請求項３０】

認証情報に加えて暗号鍵を発行することを特徴とする請求項２７に記載のコン

テンツ監視方法。

【請求項３１】

使用中のコンテンツを取得して認証情報の有無を検査するステップを具備することを特徴とする請求項２７に記載のコンテンツ監視方法。

【請求項３２】

コンテンツ使用者のコンテンツ使用履歴を基にコンテンツ使用状況を管理するステップを具備することを特徴とする請求項２７に記載のコンテンツ監視方法。

【請求項３３】

所定の権利者から許諾を受けてコンテンツを使用するコンテンツ使用装置であって、

コンテンツの使用許諾を示す認証情報を外部から受け取る受信手段と、

該受け取った認証情報を付けてコンテンツを使用する使用手段と、

を具備することを特徴とするコンテンツ使用装置。

【請求項３４】

前記使用手段は、認証情報を付けたコンテンツを所定の配布路経由で配布することを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項３５】

前記認証情報は、少なくとも、現在時刻を示す時刻識別情報と自身に対して割り当てられた使用者識別情報を含むことを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項３６】

前記認証情報は、少なくとも、配布者に対して割り当てた配布者識別情報と、該配布者におけるコンテンツの使用履歴をアドレス可能な識別情報を含むことを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項３７】

前記受信手段は、認証情報に加えて暗号鍵を受け取り、

前記使用手段は、該暗号鍵を用いて暗号化した認証情報を付けてコンテンツを使用する、

ことを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項３８】

前記使用手段は、電子透かし技術を用いて認証情報をコンテンツに埋め込むことを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項３９】

前記使用手段は、電子透かし技術を用いて認証情報をコンテンツの使用信号に埋め込むことを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項４０】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、前記使用手段において使用された各コンテンツの使用履歴をコンテンツ識別情報と関連付けて保存する履歴情報格納手段を具備することを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項４１】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、

前記使用手段において使用された各コンテンツの使用履歴をコンテンツ識別情報と関連付けて保存する履歴情報格納手段と、

該保存された使用履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを前記履歴情報格納手段から抽出する履歴情報抽出手段と、

を具備することを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項４２】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、

前記使用手段において使用された各コンテンツの使用履歴をコンテンツ識別情報と関連付けて保存する履歴情報格納手段と、

該保存された使用履歴を基に各コンテンツの使用状況を管理する使用状況管理手段と、

を具備することを特徴とする請求項３３に記載のコンテンツ使用装置。

【請求項４３】

所定の権利者から許諾を受けてコンテンツを使用するコンテンツ使用方法であ

って、

コンテンツの使用許諾を示す認証情報を外部から受け取る受信ステップと、

該受け取った認証情報を付けてコンテンツを使用する使用ステップと、

を具備することを特徴とするコンテンツ使用方法。

【請求項４４】

前記使用ステップでは、認証情報を付けたコンテンツを所定の配布路経由で配布することを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項４５】

前記認証情報は、少なくとも、現在時刻を示す時刻識別情報と自身に対して割り当てられた使用者識別情報を含むことを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項４６】

前記認証情報は、少なくとも、配布者に対して割り当てた配布者識別情報と、該配布者におけるコンテンツの使用履歴をアドレス可能な識別情報を含むことを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項４７】

前記受信ステップでは、認証情報に加えて暗号鍵を受け取り、

前記使用ステップでは、該暗号鍵を用いて暗号化した認証情報を付けてコンテンツを使用する、

ことを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項４８】

前記使用ステップでは、電子透かし技術を用いて認証情報をコンテンツに埋め込むことを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項４９】

前記使用ステップでは、電子透かし技術を用いて認証情報をコンテンツの使用信号に埋め込むことを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項５０】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、前記使用ステップにおいて使用された各コンテンツの使用履歴をコン

テンツ識別情報と関連付けて保存する履歴情報格納ステップを具備することを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項５１】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、

前記使用ステップにおいて使用された各コンテンツの使用履歴をコンテンツ識別情報と関連付けて保存する履歴情報格納ステップと、

該保存された使用履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを抽出する履歴情報抽出ステップと、

を具備することを特徴とする請求項４３に記載のコンテンツ使用方法。

【請求項５２】

各コンテンツは固有のコンテンツ識別情報を有し、

さらに、

前記使用ステップにおいて使用された各コンテンツの使用履歴をコンテンツ識別情報と関連付けて保存する履歴情報格納ステップと、

該保存された使用履歴を基に各コンテンツの使用状況を管理する使用状況管理ステップと、

を具備することを特徴とする請求項４３に記載のコンテンツ使用方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、遠隔地間でコンテンツを配信・配布若しくは提供するためのコンテンツ配信技術に係り、特に、例えば放送波やネットワーク転送の形式で多数人に対してコンテンツを配信・配布若しくは提供するためのコンテンツ配信技術に関する。

【０００２】

更に詳しくは、本発明は、音楽や映像などのようにコンテンツ作成者等が著作権を始めとする所定の使用権を有するコンテンツを安全に配信・配布若しくは提供するためのコンテンツ配信技術に係り、特に、コンテンツに関する権利者等が

コンテンツの配信・配布若しくは提供状況を好適に管理又は監視するためのコンテンツ配信技術に関する。

【０００３】

【従来の技術】

著作権とは、著作物を利用し得る相対的な排他的独占権であり、いわゆる無体財産権の１つに含まれる。ここで言う「著作物」とは、思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するものを指す。著作権は、例えば、各国の著作権法や、ベルヌ条約や万国著作権条約などの国際的な条約で保護されている。

【０００４】

著作権の利用は、著作権者自身において行われるのはごく稀であり、他人が著作権を利用することに対して一定の対価を得て許諾するのが一般的である。例えば、楽曲などの音楽コンテンツに関する著作権を所有するレコード会社などは、音楽コンテンツを使用すなわち放送する放送局やコンテンツ配信業者に対して、コンテンツ使用回数に応じた著作権使用料を要求することができる。

【０００５】

昨今、情報処理及び情報通信技術が飛躍的に進歩するとともに、文化的及び経済的な分野においては国際化が目覚しく進展してきた。かかる社会環境下では、著作権をめぐる情勢も刻々と変貌してきている。著作権保護の歴史は１５世紀中ごろの印刷技術の発明に由来すると言われているが、現在では、あらゆるデータやコンテンツがデジタル化して計算機システム上で取り扱うことが可能となり、これと相俟って、著作物の複製もますます容易になってきた。したがって、情報技術の観点からも著作物の正当な利用を支援し若しくは不正利用を排除して、著作権の保護を拡充する必要があると思料される。

【０００６】

デジタル・コンテンツの世界において、不正コピーに対抗するための１つの手段として「電子透かし」（Ｄｉｇｉｔａｌ　Ｗａｔｅｒｍａｒｋｉｎｇ　又はＤａｔａ　Ｈｉｄｉｎｇとも言う）と呼ばれる技術を挙げることができる。電子透かしとは、画像や音楽などのコンテンツ中に、ほとんど目に見えない又は耳に聞

こえない形で情報を埋め込むことを意味する。例えば、著作権情報を電子透かしにより埋め込むことで、後にコンテンツを採取したときに、透かしすなわち著作権情報を浮き上がらせて、データの流通経路や使用権の有無を検査することができる。

【０００７】

例えば、音楽レコード業界及び放送業界において、各楽曲毎に一意に付与される識別情報であるＩＳＲＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｓｔａｎｄａｒｄ　Ｒｅｃｏｒｄｉｎｇ　Ｃｏｄｅ）を著作権情報としてあらかじめ音楽コンテンツに埋め込むことで著作物の使用を自動管理する、という試みが検討されている。

【０００８】

著作権者としての音楽レコード会社と著作権利用者としての放送局との間では、例えば、各楽曲毎に放送した回数分だけの著作権使用料を支払うような契約が取り交わされている。したがって、音楽レコード会社（若しくはレコード会社から委託を受けた監視会社）は、放送波を受信して埋め込まれた電子透かしを解読して、ＩＳＲＣの出現を基にして各楽曲毎の使用回数を計数することができる。また、放送局側が著作権使用料を正確又は正直に申告してこなくても、計数値を基に音楽レコード会社は不正な申告をあばくことができるし、必要に応じて著作権使用契約を解除するなどのペナルティを課すこともできるであろう。

【０００９】

ＩＳＲＣを活用して著作権の使用を徹底的に取り締まるためには、ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ）などの記憶媒体上に音楽コンテンツを格納する（すなわち製造する）時点で、各楽曲毎にＩＳＲＣを埋め込んでおくことが好ましい。

【００１０】

しかしながら、上述した方式に頼ると、電子透かしを埋め込む以前の従来のＣＤから再生された音楽コンテンツの利用を追跡したり監視したりすることはできない。また、既存のコンテンツをすべて電子透かし入りの新しいコンテンツに置き換えることは不可能に等しい。

【００１１】

また、すべてのコンテンツに電子透かしを入れるには、音楽だけで６０ビット

のデータ・フィールドを必要とし、全体のコード長が著しく増大してしまう。

【００１２】

【発明が解決しようとする課題】

本発明の目的は、例えば放送波やネットワーク転送の形式で多数人に対してコンテンツを配信・配布若しくは提供することができる、優れたコンテンツ配信技術を提供することにある。

【００１３】

本発明の更なる目的は、音楽や映像などのようにコンテンツ作成者等が著作権を始めとする所定の使用権を有するコンテンツを安全に配信・配布若しくは提供することができる、優れたコンテンツ配信技術を提供することにある。

【００１４】

本発明の更なる目的は、コンテンツに関する権利者等がコンテンツの配信・配布若しくは提供状況を好適に管理又は監視し、コンテンツ使用料を正確に課すことができる、優れたコンテンツ配信技術を提供することにある。

【００１５】

本発明の更なる目的は、既に流通後の記録媒体から再生されたコンテンツに対しても、コンテンツの配信・配布若しくは提供状況を好適に管理又は監視することができる、優れたコンテンツ配信技術を提供することにある。

【００１６】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、所定の権利者が所有するコンテンツを提供するためのコンテンツ提供システムであって、

コンテンツの使用許諾を示す認証情報を発行してコンテンツの提供を監視する監視装置と、

前記監視装置から受け取った認証情報を付けてコンテンツを所定の配布路経由で提供する配布装置と、

を具備することを特徴とするコンテンツ提供システムである。

【００１７】

ここで言う監視装置は、例えばコンテンツの著作権を所有する著作権者、又は、著作権者からコンテンツ使用の監視業務を受けた者が運営する装置である。これに対し、配布装置は、著作権者からコンテンツの使用許諾を受けた業者が運用する装置である。監視装置と配布装置とは、認証情報や、その他の後述する各種情報を安全に交換するために、専用線などの安全な伝送媒体で相互接続されていることが好ましい。

【００１８】

後述する実施例では、コンテンツ配布業者としての放送局が放送波によってコンテンツを配信する場合を使用する場合を例にとって説明する。但し、本発明で言う配布は、「放送」には限定されず、例えば、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やインターネットを経由したネットワーク配信サービスや、ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｃ）やＭＯ（Ｍａｇｎｅｔｏ－Ｏｐｔｉｃａｌ　ｄｉｓｃ）ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）など各種の記憶媒体を介したコンテンツ流通を行う場合であっても、同様に利用することができると理解されたい。

【００１９】

前記監視装置は、前記所定の配布路上で提供中のコンテンツを取得して、該コンテンツに認証情報が付されているか否かで配布装置によるコンテンツ提供行為の正当性を判断することができる。

【００２０】

また、前記監視装置が発行する認証情報は、現在時刻を示す時刻識別情報と、配布装置に対して割り当てた配布者識別情報の組で構成されていてもよい。

【００２１】

また、前記監視装置は、認証情報に加えて暗号鍵を発行してもよい。このような場合、前記配布装置は、前記監視装置から受け取った暗号鍵を用いて暗号化した認証情報を付けてコンテンツを前記所定の配布路経由で提供することができる。したがって、配布路上で、コンテンツに添付された認証情報の改竄を好適に防止することができる。

【００２２】

また、前記配布装置は、電子透かし技術を用いて認証情報をコンテンツに埋め込んでもよい。あるいは、前記配布装置は、電子透かし技術を用いて認証情報をコンテンツの配布信号に埋め込んでもよい。電子透かし技術を用いることにより、放送波を受信する一般視聴者は、認証情報の存在を意識させずに済む。特に後者の場合には、コンテンツ自体に認証情報を埋め込む必要がないので、既に流通された記憶媒体から再生された音楽コンテンツに対しても容易に認証情報を埋め込むことができる。

【００２３】

通常、各コンテンツは固有のコンテンツ識別子を備えている。例えば、音楽コンテンツであれば、各楽曲には、国際レベルで識別可能なＩＳＲＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｓｔａｎｄａｒｄ　Ｒｅｃｏｒｄｉｎｇ　Ｃｏｄｅ）が割り振られている。

【００２４】

前記配布装置は、前記所定の配布路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存することができる。

【００２５】

また、前記監視装置は、該提供履歴をアドレス可能な識別情報を前記認識情報に含めるようにしてもよい。この場合、時刻識別情報を認識情報に含めなくてもよい。

【００２６】

また、配布装置は、該提供履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを抽出して、監視装置などの監視業者に渡すことができる。前述のＩＳＲＣの場合、１～５の５個のグループで構成されるが、そのうちグループ３に相当する３桁は第一所有者（ｆｉｒｓｔ　ｏｗｎｅｒ　ｃｏｄｅ）を示す。このグループ３をマスクに用いてフィルタリングすることにより、特定の著作権者のコンテンツに関する提供履歴情報のみを抽出することができる。これに対し、監視装置側では、提供履歴情報を基にして、各コンテンツの提供状況を管理することができる。例えば、コンテンツの使用回数に応じた正確な著作権使用料を、配布装置すなわち放送局に対して課金することができる。

【００２７】

また、本発明の第２の側面は、所定の権利者が所有するコンテンツを提供するためのコンテンツ提供方法であって、

コンテンツの使用許諾を示す認証情報を発行する第１のステップと、

前記第１のステップにおいて発行された認証情報を付けてコンテンツを所定の配布路経由で提供する第２のステップと、

前記配布路上におけるコンテンツの提供を監視する第３のステップと、

を具備することを特徴とするコンテンツ提供方法である。

【００２８】

前記第３のステップでは、前記所定の配布路上で提供中のコンテンツを取得して、該コンテンツに認証情報が付されているか否かでコンテンツ提供行為の正当性を判断することができる。

【００２９】

また、前記第１のステップでは、現在時刻を示す時刻識別情報とコンテンツ配布に対して割り当てた配信者識別情報の組を認証情報として発行してもよい。

【００３０】

また、前記第１のステップでは、認証情報に加えて暗号鍵を発行してもよい。この場合、前記第２のステップでは、前記第１のステップにおいて発行された暗号鍵を用いて暗号化した認証情報を付けてコンテンツを前記所定の配布路経由で提供することができ、認証情報の改竄を好適に防止することができる。

【００３１】

また、前記第２のステップでは、電子透かし技術を用いて認証情報をコンテンツに埋め込むようにしてもよい。あるいは、前記第２のステップでは、電子透かし技術を用いて認証情報をコンテンツの配布信号に埋め込むようにしてもよい。

【００３２】

各コンテンツは、通常、固有のコンテンツ識別情報を有している。このような場合、前記第２のステップにおいて前記所定の配信路経由で提供する各コンテンツの提供履歴をコンテンツ識別情報と関連付けて保存する第４のステップをさらに具備することができる。また、該提供履歴をアドレス可能な識別情報を前記認

識情報に含めるようにしてもよい。この場合、時刻識別情報を認識情報に含めなくてもよい。また、該提供履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを抽出する第５のステップや、該提供履歴を基に各コンテンツの提供状況を管理する第６のステップを備えていてもよい。

【００３３】

また、本発明の第３の側面は、所定の権利者が所有するするコンテンツの使用を監視するためのコンテンツ監視装置又は方法であって、コンテンツ使用者に対して使用許諾を示す認証情報を発行する手段を具備することを特徴とするコンテンツ監視装置又は方法である。

【００３４】

また、前記認証情報は、少なくとも、現在時刻を示す時刻識別情報と配布者に対して割り当てた配布者識別情報を含んでもよい。

【００３５】

また、認証情報に加えて暗号鍵を発行するようにしてもよい。

【００３６】

また、使用中のコンテンツを取得して認証情報の有無を検査する手段又はステップをさらに備えてもよい。

【００３７】

また、コンテンツ使用者のコンテンツ使用履歴を基にコンテンツ使用状況を管理する手段又はステップをさらに備えてもよい。

【００３８】

また、本発明の第４の側面は、所定の権利者から許諾を受けてコンテンツを使用するコンテンツ使用装置又は方法であって、

コンテンツの使用許諾を示す認証情報を外部から受け取る受信手段又はステップと、

該受け取った認証情報を付けてコンテンツを使用する使用手段又はステップと、

を具備することを特徴とするコンテンツ使用装置又は方法である。

【００３９】

前記使用手段又はステップは、認証情報を付けたコンテンツを所定の配布路経由で配布することができる。この結果、配布路上の使用コンテンツに認証情報が含まれているか否かによって該コンテンツの正当性を検査することができる。

【００４０】

前記認証情報は、少なくとも、現在時刻を示す時刻識別情報と自身に対して割り当てられた使用者識別情報を含むことができる。

【００４１】

また、前記受信手段又はステップは認証情報に加えて暗号鍵を受け取り、前記使用手段又はステップは該暗号鍵を用いて暗号化した認証情報を付けてコンテンツを使用するようにしてもよい。この結果、配布路上で認証情報の改竄を好適に防止することができる。

【００４２】

また、前記使用手段は、電子透かし技術を用いて認証情報をコンテンツに埋め込むようにしてもよい。あるいは、前記使用手段又はステップは、電子透かし技術を用いて認証情報をコンテンツの使用信号に埋め込んでもよい。

【００４３】

各コンテンツは、通常、固有のコンテンツ識別情報を備えている。したがって、履歴情報格納手段又はステップは、前記使用手段又はステップにおいて使用された各コンテンツの使用履歴をコンテンツ識別情報と関連付けて保存することができる。また、該使用履歴をアドレス可能な識別情報を前記認識情報に含めるようにしてもよい。この場合、時刻識別情報を認識情報に含めなくてもよい。

【００４４】

また、該保存された使用履歴を所定のフィルタでマスクして特定のコンテンツに関連のある履歴情報のみを抽出することができる。また、該保存された使用履歴を基に各コンテンツの使用状況を管理することもできる。

【００４５】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４６】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施例を詳解する。

【００４７】

図１には、本発明に係るコンテンツ配信システム１００の概念を模式的に示している。同図に示すように、該コンテンツ配信システム１００は、放送局１０と監視局５０とで構成される。

【００４８】

監視局５０は、著作権者自身が運営するか、若しくは、著作権者から委託を受けて著作物の使用を追跡又は監視する団体・会社によって運営される。著作権者は、音楽コンテンツを例えばＣＤのような記録媒体上に格納して販売・流通する音楽レコード会社である。また、監視局５０は、放送局が放送に利用する各コンテンツすなわち著作物のを監視するが、その詳細な手順については後述に譲る。

【００４９】

図１に示す例では、各著作権者毎に監視局が設定されているが、図２に示すように単一の監視局が複数の著作権者に対してコンテンツ利用の監視サービスを提供してもよい。

【００５０】

また、実世界上には放送局は複数存在し、著作権者はすべての放送局に対して自らの著作物すなわちコンテンツの利用状況を監視しなければならない。著作権者は、各放送局毎に監視局を設立してもよいし、あるいは、単一の監視局が複数の放送局をカバーしてもよい。

【００５１】

以下では、便宜上、１つの監視局５０が１つの放送局１０を監視する場合を例にとって説明することにする。

【００５２】

放送局１０と監視局５０の間は、専用線２０などの安全な伝送路を介して相互接続されており、所定の認証手続きを経ることでいわゆる「なりすまし」を排除することができる。

【００５３】

両者間で認証が確立している間、監視局５０は、放送局１０に対して、放送局識別情報（以下、「放送局ＩＤ」とする）と、時刻識別情報（以下、「時刻ＩＤ」とする）と、暗号用の鍵を供給する。以下では、放送局ＩＤと時刻ＩＤの組み合わせで構成される情報を「認証情報」と呼ぶことにする。認証情報は、コンテンツに関する使用許諾を証明する能力を持つ。

【００５４】

但し、認証情報に時刻識別情報を必ずしも含める必要はない。例えば、放送局において蓄積される放送履歴情報（後述）の各レコードをアドレス可能な他の識別情報に置き換えることもできる。

【００５５】

【数１】

［　放送局ＩＤ　］：［　時刻ＩＤ　］：［　鍵　］

【００５６】

放送局ＩＤは、著作権者を代行する監視局５０が放送局１０を認証し、さらには著作物の使用を許諾したことの証しでもある。監視局５０が定常的又は固定的に著作物の使用を許諾するときには、監視局５０は、認証確立後にただ１度だけ放送局ＩＤを放送局１０に転送すればよい。一方、著作物の使用を時限的にのみ許諾する場合には、認証が確立された期間中で、新たに著作物の使用を許諾する度に、新しい放送局ＩＤを放送局１０に転送する必要がある。時限的な放送局ＩＤは、例えば後述の時刻ＩＤと組にして管理することができる。後者の運用形態の場合、監視局５０は、例えば、放送番組毎又は放送時間帯毎に著作物の使用許諾を与えることができる。

【００５７】

また、時刻ＩＤは、現在時刻と一意な関係にある識別情報であり、例えば時刻データそのものであってもよい。監視局５０による時刻ＩＤの付与と、放送局１０におけるコンテンツ配信すなわち番組放送がリアルタイムで行われている場合（あるいは、時刻ＩＤの付与とコンテンツ配信のタイムラグが一定値である場合）には、時刻ＩＤは番組の放送時刻や放送されたコンテンツ自体を特定することができる。

【００５８】

鍵は、放送局１０側において、放送局ＩＤや時刻ＩＤからなる所定の認証情報を暗号化し、さらに、監視局５０において暗号情報を解読するために使用される暗号鍵のことである。１つの鍵を固定的に使用する場合には、監視局５０は、認証確立後にただ１度だけ鍵を放送局１０に転送すればよい。但し、鍵の使い回しを防止するために、監視局５０は、時間の経過とともに鍵を変更し、且つ、変更する度に放送局１０側に鍵を転送しなければならない。後者の場合、鍵を時間的な関数Ｋｅｙ（ｔ）として把握することができる。また、Ｋｅｙ（ｔ）は、時刻ＩＤと関連付けて管理しておけばよい。

【００５９】

なお、ここで使用する鍵は、暗号時及び解読時に同じ鍵を用いる共通鍵暗号方式、又は、秘密鍵と公開鍵の組み合わせで構成される公開鍵暗号方式のいずれであってもよい。但し、以下の説明では、便宜上、共通鍵であるとする。

【００６０】

放送局１０側では、放送コンテンツに対して、監視局５０から受け取った認証情報を重畳した放送波を生成して、各受信機に向けて伝送すなわち放送する。

【００６１】

認識情報は、上述したように、放送局ＩＤと時刻ＩＤの組み合わせ（例えば、各ＩＤをビット連結させたもの）で構成される。監視局１０による認証とリアルタイムで放送する場合には、時刻ＩＤを省略することができる。但し、受信者側において放送コンテンツを記録媒体上に格納したものに対してその出所すなわち著作物の著作権者を特定するためには、時刻ＩＤを認証情報の一部に使用することが好ましい。

【００６２】

本発明を実現する上で、認証情報を放送コンテンツに添付する形態は特に問わない。例えば、電子透かし技術を用いて放送局ＩＤ及び時刻ＩＤを重畳してもよい。このような場合、コンテンツ自体、あるいは、放送波のいずれに対して認証情報を重畳してもよい。電子透かし技術を利用することにより、一般の視聴者等の受信者は、認証情報の存在を全く気にしなくて済む。

【００６３】

元のコンテンツではなく、放送波に対して電子透かしを行う場合、放送局の設備を変更するだけで、本発明を適用することができる。また、コンテンツそのものに電子透かしを入れる必要がないので、既に普及されているＣＤなどの記録媒体を源とするコンテンツに対しても、好適に著作権管理を行うことができる。

【００６４】

また、電子透かしによって埋め込まれた認証情報を改竄から保護するために、監視局５０から受け取った鍵を用いて、放送局ＩＤ及び時刻ＩＤからなる認証情報を暗号化してから（図３（ａ）を参照のこと）、放送波に重畳するようにしてもよい。このような場合、監視局５０側では認証情報を解読する必要がある。さらに鍵が時間の関数Ｋｅｙ（ｔ）である場合には、監視局５０はどの鍵を用いて解読すべきかを特定しなければならない。したがって、暗号化された認証情報にさらに平文形式の時刻ＩＤを添付した情報（図３（ｂ））を、放送波に重畳するとよい。監視局５０側では、時刻ＩＤを基に、該当する鍵Ｋｅｙ（ｔ）を特定することができる。

【００６５】

また、放送局１０は、自身が放送したコンテンツに関する放送履歴情報を蓄積し、データベース管理する。該データベースは、放送したコンテンツ毎にレコードを作成することが好ましく、各レコードは、以下に示すように、少なくともコンテンツＩＤ、時刻ＩＤ、及び放送局ＩＤの各々を格納するフィールドを備えている。

【００６６】

【数２】

［　コンテンツＩＤ　］：［　時刻ＩＤ　］：［　放送局ＩＤ　］

【００６７】

ここで言うコンテンツＩＤは、放送コンテンツを一意に識別可能な情報である。例えば音楽コンテンツであれば、ＩＳＯ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｏｒｇａｎｉｚａｔｉｏｎ　ｆｏｒ　Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ）３９０１において規定されているＩＳＲＣを利用することができる。また、コマーシャルで

あれば、ＩＳＣＩを利用することができる。これら以外に、例えばシーケンスに貼り付けたタグをコンテンツＩＤとして使用することができる。

【００６８】

データベース化された履歴情報は、監視局５０に対して適宜（例えば要求に応答して）転送される。若しくは、監視局５０は、自律的に履歴情報データベースに対してアクセス可能である。

【００６９】

図４には、本実施例に係るコンテンツ配信システム１００の構成をより具体的に示している。

【００７０】

同図に示すように、監視局５０側は、監視サーバ５１と、現在時刻を提供する時計５２と、放送局１０の放送波を受信する１以上の受信機５３Ａ，５３Ｂで構成される。監視サーバ５１は、暗号化通信などの安全な通信方式により各部と接続されているものとする。

【００７１】

監視サーバ５１は、管理サーバ１１とは専用線２０などの安全な伝送路で相互接続されており、所定の手続きに従って監視局５０と放送局１０との間で認証を確立することができる。認証を確立した結果、監視サーバ５１は、放送局１０に対して放送局ＩＤや時刻ＩＤなどの認証情報と、鍵を供給することができる。

【００７２】

また、放送局１０側は、局内の動作を統括的に管理する管理サーバ１１と、再生機１２と、編集機１３と、放送サーバ１４と、電子透かし埋め込み部１５と、送信機１６と、放送履歴データベース１７で構成される。管理サーバ１１は、暗号化通信などの安全な通信方式により各部と接続されているものとする。

【００７３】

再生機１２は、音楽や映像、アナウンスなどメディアを再生する。また、編集機１３は、再生された各メディアを統合・編集して放送コンテンツを編集する。編集結果は、放送サーバ１４において蓄積される。

【００７４】

放送サーバ１４は、暗号化通信などの安全な通信方式により、管理サーバ１１と常時接続されている。そして、メディア再生、放送コンテンツ編集及び記録などに関する放送履歴を放送履歴情報データベース１７上に安全に保管することができる。履歴情報データベース１７上には、例えば放送コンテンツ毎にレコードが作成され、各レコードは少なくともコンテンツＩＤ、時刻ＩＤ、及び放送局ＩＤの各々を格納するフィールドを備えている。（前述）。

【００７５】

また、放送サーバ１４は、編集機１３による編集成果物を放送波として配信可能な形式まで仕上げて、管理サーバ１１によって制御された予定時刻（例えば放送時刻）にこれを出力する。

【００７６】

電子透かし埋め込み部１５は、監視サーバ５１から受け取った認証情報を、電子透かしとして埋め込む。認証情報は、放送局ＩＤと時刻ＩＤで構成される。この際、認証情報の改竄を防止するために、監視サーバ５１から受け取った鍵を用いて認証情報を暗号化してから埋め込むことが好ましい。また、セキュリティ・レベルを向上させるためには、鍵を時間とともに変化させることが好ましいが、この場合、使用した鍵を特定しやすくするために、暗号化された認証情報に平文形式の時刻ＩＤを添付したものを埋め込むとよい（前述及び図３（ｂ）を参照のこと）。

【００７７】

送信機１１は、上述のようにして認証情報が埋め込まれた放送波を発射する。但し、放送波は、地上波であっても衛星波であってもよいし、伝送路は無線又は有線いずれであってもよい。また、本発明の変形例として、コンテンツ配信の経路は、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やインターネットなどのネットワーク、あるいは、ＰＳＴＮ（Ｐｕｂｌｉｃ　Ｓｗｉｔｃｈｅｄ　Ｔｅｌｅｐｈｏｎｅ　Ｎｅｔｗｏｒｋ）やＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ　Ｓｅｒｖｉｃｅｓ　Ｄｉｇｉｔａｌ　Ｎｅｔｗｏｒｋ）などの公衆電話網によるコンテンツ配信・流通であっても構わない。また、コンテンツ配信形態は、プッシュ型又はプル型のいずれであってもよい。

【００７８】

管理サーバ１１は、監視サーバ５１とは専用線などの安全な伝送路で相互接続されており、所定の手続きに従って監視局５０と放送局１０との間で認証を確立することができる。認証を確立した結果、管理サーバ１１は、監視サーバ５１に対して、放送履歴情報データベース１７に蓄積された履歴情報を適宜（例えば要求に応答して）転送することができる。若しくは、監視サーバ５１は、履歴情報データベースに対してアクセス可能である。

【００７９】

放送局１０は、通常、複数の著作権者のコンテンツを利用して放送番組を制作する。また、図１に示したように、１つの放送局１０が、各著作権者毎に設定された複数の監視局５０の監視下に置かれる場合もある。このような場合には、放送履歴情報データベース１７に蓄積されたすべてのレコードをすべての監視局５０Ａ，５０Ｂ…に対して送信するのは非効率的且つ非合理的である。何故ならば、著作権者以外に著作物の使用状況を開示することはプライバシ侵害に相当し、また、余分なデータ転送は通信負荷をいたずらに増大させることになるからである。したがって、各著作権者毎に履歴情報をフィルタリングしてから、監視局５０に送信すべきである。

【００８０】

例えば、音楽コンテンツに対して割り当てられるＩＳＲＣの場合、１～５の５個のグループで構成されるが、そのうちグループ３に相当する３桁は第一所有者（ｆｉｒｓｔ　ｏｗｎｅｒ　ｃｏｄｅ）を示す。このグループ３をマスクに用いてフィルタリングすることにより、特定の著作権者のコンテンツに関する履歴情報のみを抽出することができる。これに対し、監視局５０側では、履歴情報を基にして、各コンテンツの提供状況を管理することができる。例えば、コンテンツの使用回数に応じた正確な著作権使用料を、配布装置すなわち放送局に対して課金することができる。

【００８１】

次いで、監視局５０において、著作物の使用状況を監視するための処理手順について説明する。但し、ここで言う著作物とは、放送局１０において放送番組中

で使用される音楽コンテンツを指し、著作物の使用者は放送局１０であり、監視対象は放送局１０から発射される放送波である。

【００８２】

監視用の受信機５３Ａ，５３Ｂは、放送波を受信すると、電子透かしをデコードして、認証情報を取り出し、これを監視サーバ１１に安全な形式で転送する。

【００８３】

監視サーバ１１では、認証情報が放送波に含まれていることを以って、放送局１０が著作物すなわちコンテンツを正当に使用していることを確認することができる。認証情報がコンテンツに含まれていない場合、放送局１０が著作物を正規に使用していないことを意味するので、放送局１０に対してペナルティを課してもよい。ペナルティは、例えば、コンテンツの使用権を剥奪若しくは一定期間停止するなどの措置でよい。

【００８４】

また、放送局１０が鍵で暗号化した認証情報を埋め込むようにすることで、配信経路上でのなりすましがないか否かを判断することができる。すなわち、放送コンテンツに対応する鍵で認証情報をデコードできない場合は、なりすましと判断することができる。また、図３（ｂ）に示すような形式の認証情報が埋め込まれているときには、平文で添付された時刻ＩＤと、認証情報をデコードして得られた時刻ＩＤが照合しない場合も、なりすましと判断することができる。

【００８５】

管理サーバ１１は、再生機１１から送信機１６に至る系を監視して、コンテンツが改竄されていないことを確認した後に、監視サーバ５１に対して鍵の発行を要求するようにする。この結果、放送履歴情報データベース１７には、安全が確認された放送履歴情報のみが蓄積されることになる。

【００８６】

［追補］

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【００８７】

上述した実施例では、ＩＳＲＣやシーケンスに貼り付けたタグなどをコンテンツＩＤとして電子透かしに使用しているが、特にこれに限定されない。例えば、楽曲の一部又は全部を圧縮したデータや、楽曲の一部をサンプリングしたデータを電子透かしに使用しても、同様の作用効果を奏することができる。

【００８８】

要するに、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【００８９】

【発明の効果】

以上詳記したように、本発明によれば、例えば放送波やネットワーク転送の形式で多数人に対してコンテンツを配信・配布若しくは提供することができる、優れたコンテンツ配信技術を提供することができる。

【００９０】

また、本発明によれば、音楽や映像などのようにコンテンツ作成者等が著作権を始めとする所定の使用権を有するコンテンツを安全に配信・配布若しくは提供することができる、優れたコンテンツ配信技術を提供することができる。

【００９１】

また、本発明によれば、コンテンツに関する権利者等がコンテンツの配信・配布若しくは使用状況を好適に管理又は監視することができる、優れたコンテンツ配信技術を提供することができる。

【００９２】

また、本発明によれば、既に流通後の記録媒体から再生されたコンテンツに対しても、配信・配布若しくは提供状況を好適に管理又は監視することができる、優れたコンテンツ配信技術を提供することができる。

【００９３】

本発明によれば、元のコンテンツではなく、放送波に対して電子透かしを行うことにより、放送局の設備を変更するだけで対応することができる。また、コン

テンツそのものに電子透かしを入れる必要がないので、既に普及されているＣＤなどの記録媒体を源とするコンテンツに対しても、同様の著作権管理を行うことができる。

【図面の簡単な説明】

【図１】

本発明の実施例に係るコンテンツ配信システム１００の構成を模式的に示した図である。

【図２】

本発明の実施例に係るコンテンツ配信システム１００の他の形態を模式的に示した図である。

【図３】

電子透かしにより埋め込まれる認証情報を暗号化する様子を図解したものであり、図３（ａ）は時刻ＩＤと放送局ＩＤからなる認証情報を暗号化する様子を、図３（ｂ）は暗号化された認証情報に平文形式の時刻ＩＤを添付する様子を、それぞれ示している。

【図４】

本実施例に係るコンテンツ配信システム１００の構成を詳細に示した図である。

【符号の説明】

１０…放送局

１１…管理サーバ

１２…再生機

１３…編集機

１４…放送サーバ

１５…電子透かし埋め込み部

１６…送信機

１７…放送履歴データベース

５０…監視局

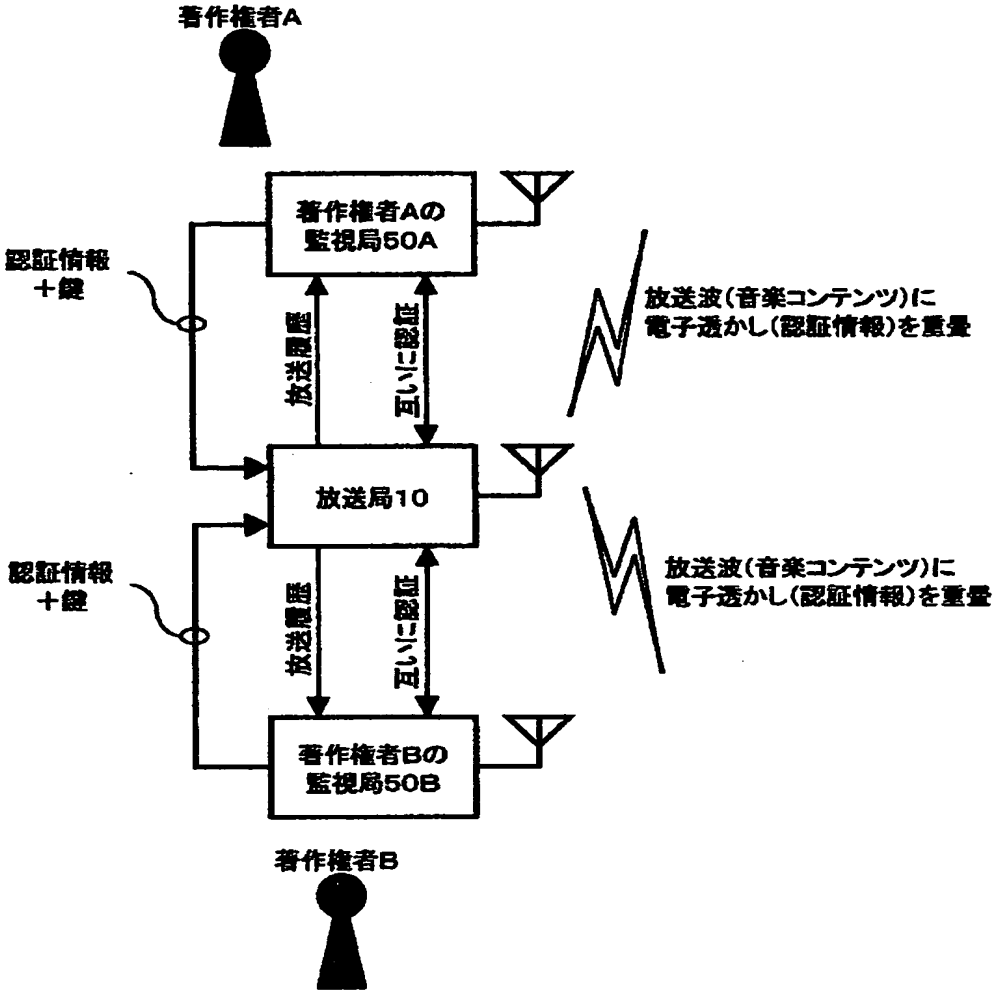
５１…監視サーバ

５２…時計

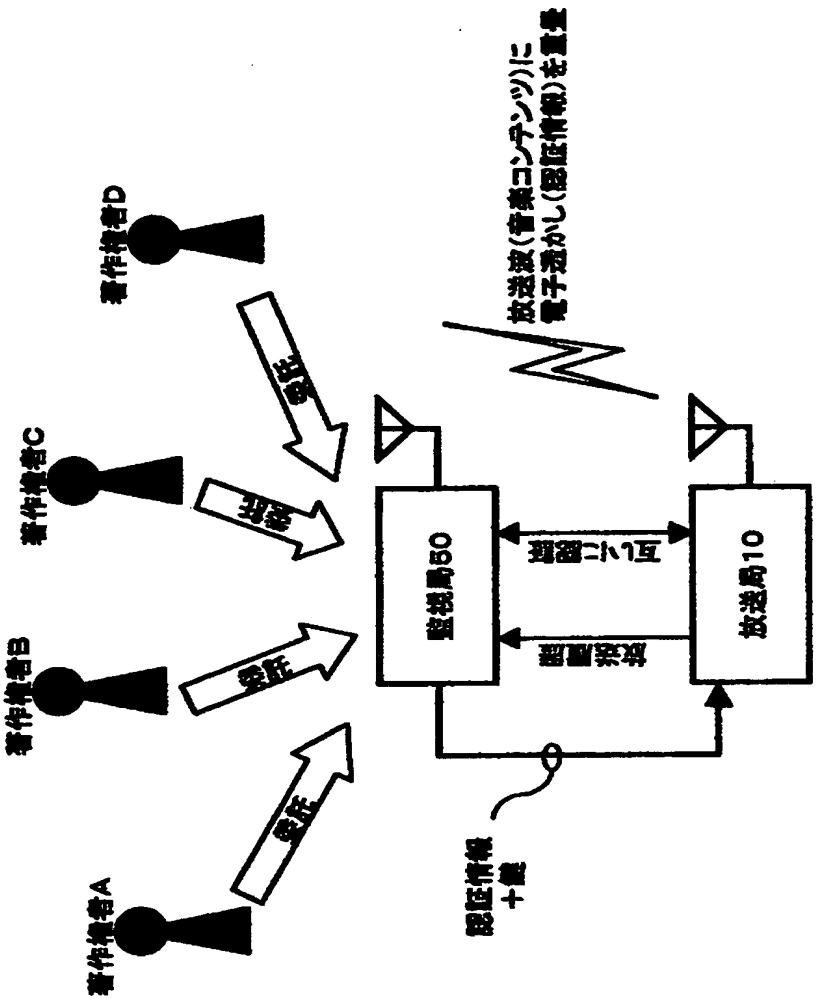
５３…受信機

【書類名】　　図面

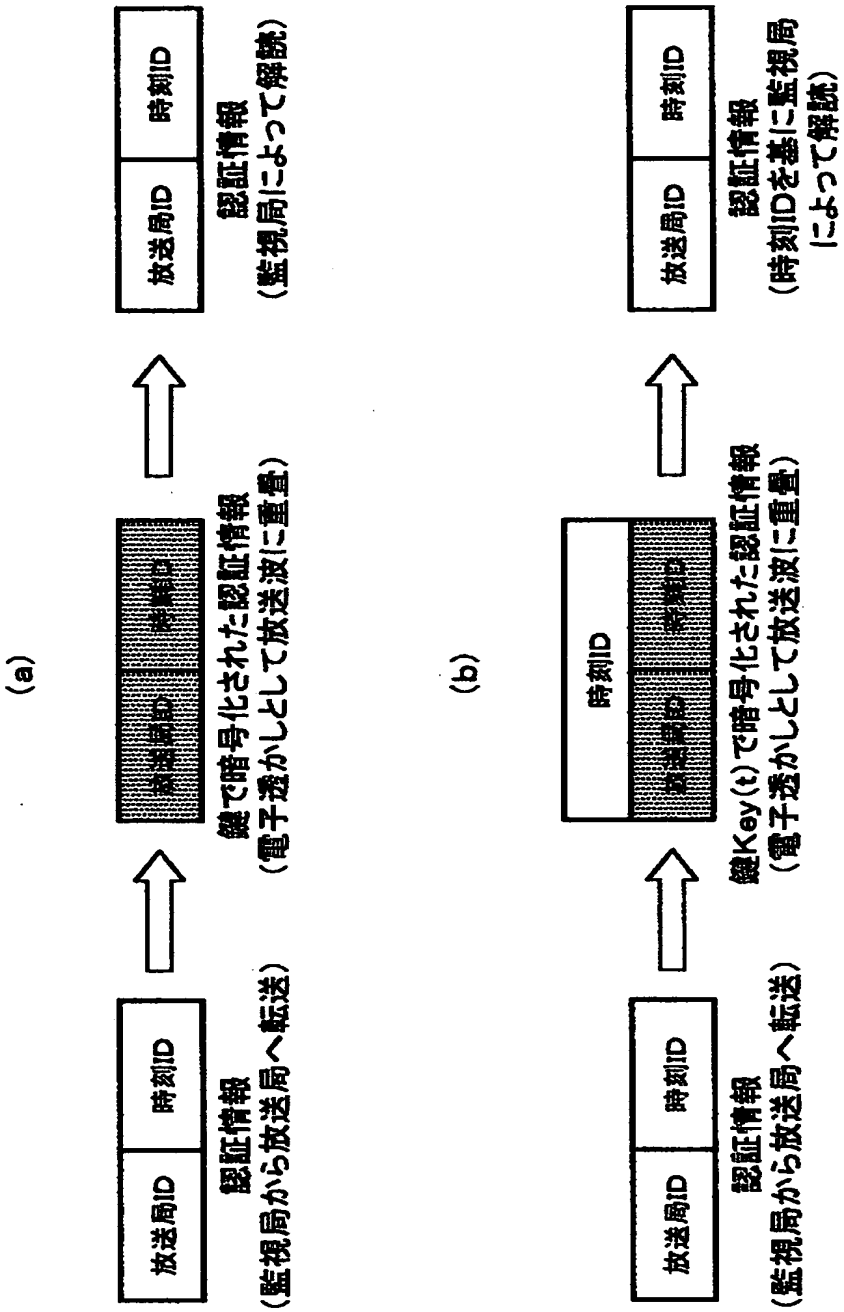
【図１】


著作権者A
著作権者Aの
監視局50A
認証情報
＋鍵
放送電波
問い合わせ
放送波(音楽コンテンツ)に
電子透かし(認証情報)を重畳
放送局10
認証情報
＋鍵
放送電波
問い合わせ
放送波(音楽コンテンツ)に
電子透かし(認証情報)を重畳
著作権者Bの
監視局50B
著作権者B

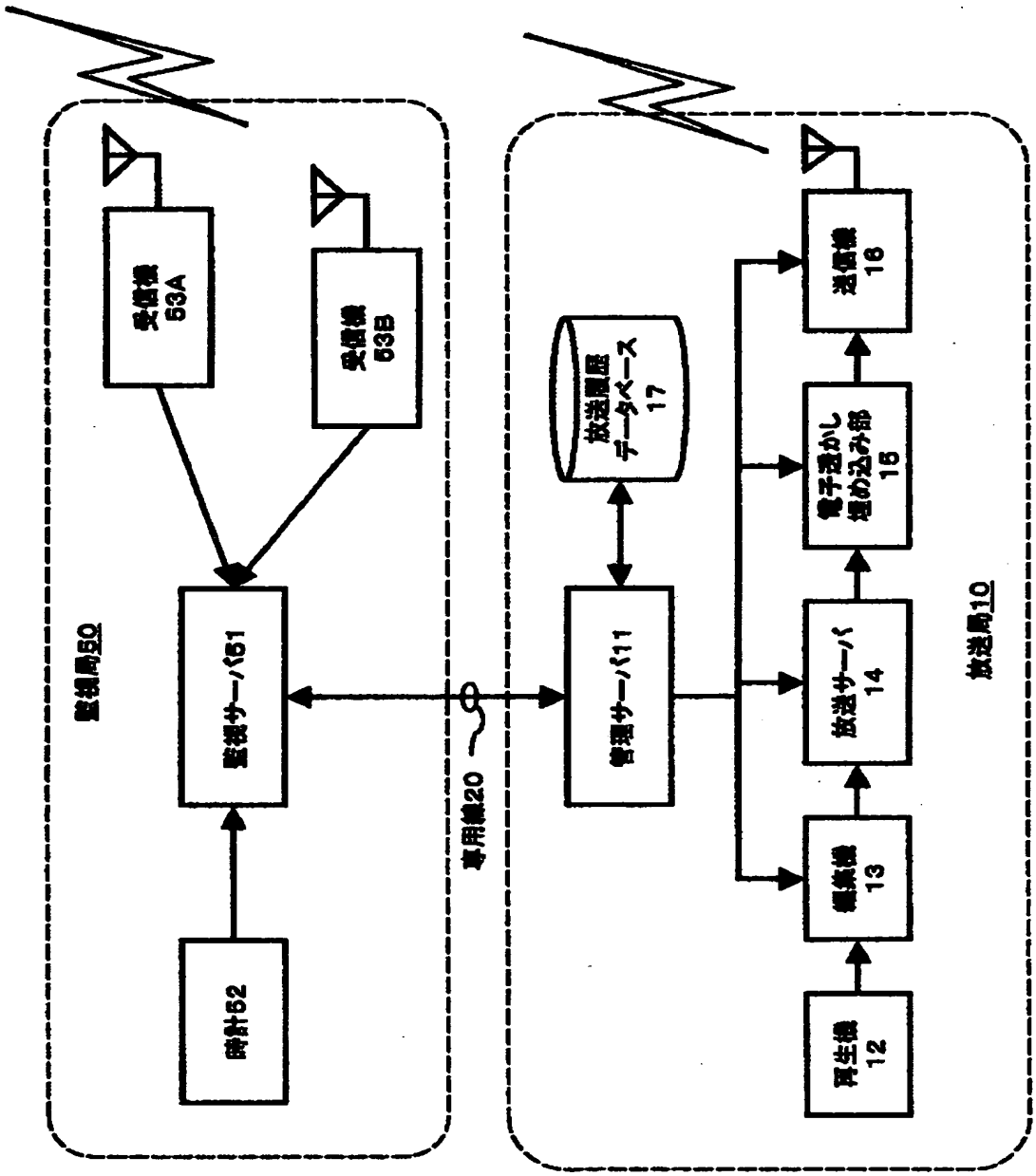
【図２】


著作権者D
著作権者C
著作権者B
著作権者A
受託
受託
受託
受託
放送局50
放送局10
互いに通知
放送通知
認証情報
＋鍵
放送(音楽コンテンツ)に
電子透かし(認証情報)を重畳

【図３】


(a)
放送局ID
時刻ID
認証情報
(監視局から放送局へ転送)
鍵で暗号化された認証情報
(電子透かしとして放送波に重畳)
放送局ID
時刻ID
認証情報
(監視局によって解読)
(b)
放送局ID
時刻ID
認証情報
(監視局から放送局へ転送)
鍵Key(t)で暗号化された認証情報
(電子透かしとして放送波に重畳)
時刻ID
放送局ID
認証情報
(時刻IDを基に監視局によって解読)

【図４】


受信機
53A
受信機
53B
監視局50
監視サーバ51
時計52
専用線20
管理サーバ11
放送履歴
データベース
17
電子透かし
埋め込み部
15
送信機
16
放送サーバ
14
編集機
13
再生機
12
放送局10

【書類名】　　要約書

【要約】

【課題】　コンテンツの配信状況を好適に管理又は監視し、コンテンツ使用料を正確に課す。

【解決手段】　コンテンツ提供システムは、コンテンツの使用許諾を示す認証情報を発行してコンテンツの提供を監視する監視装置と、認証情報を付けてコンテンツを所定の配布路経由で提供する配布装置とで構成される。認証情報は、現在時刻を示す時刻識別情報と配布装置に対して割り当てた配布者識別情報の組で構成される監視装置は、配布路上で提供中のコンテンツを取得して、該コンテンツに認証情報が付されているか否かで提供コンテンツの正当性を判断できる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社